Health Lawyers Weekly

December 20, 2013 Vol. XI Issue 49

Is Your Photocopier HIPAA Compliant?

By Jennifer Mitchell & Stacey Borowicz, Dinsmore & Shohl LLP

With contributions by Matthew Arend and Simi Botic, Dinsmore & Shohl LLP

Digital copiers have been capable of storing information, including protected health information (PHI), for over a decade. However, it wasn't until this year that the U.S. Department of Health and Human Services (HHS) announced its first Health Insurance Portability and Accountability Act of 1996 (HIPAA) breach settlement resulting from a digital photocopier.

On August 14, 2013, HHS entered into a $1,215,780 settlement with Affinity Health Plan (Affinity), a not-for-profit managed care plan servicing the New York metropolitan area, for a potential HIPAA violation arising from the lease of a digital photocopier.[1] Digital photocopiers often contain hard drives, which store all of the information that is copied. For health care providers, this information may include medical records and other documents containing PHI (i.e. driver's licenses and Social Security cards).

Under the Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Rule (Breach Notification Rule), HIPAA-covered entities must notify HHS of a breach of unsecured PHI.[2] On April 15, 2010, pursuant to the Breach Notification Rule, Affinity filed a breach report with the HHS Office for Civil Rights (OCR). The report divulged that Affinity had impermissibly disclosed the PHI of up to 344,579 individuals after returning leased photocopiers without wiping the hard drives clean.[3] After purchasing a photocopier previously leased by Affinity, CBS uncovered PHI on the machine's hard drive.[4] A CBS Evening News representative contacted Affinity to inform the HIPAA-covered entity that PHI had been disclosed.[5] As a result, OCR began an investigation of potential violations of the HIPAA Privacy and Security Rules.[6] The investigation revealed a failure by Affinity to assess potential security risks and to

implement an acceptable digital use policy relating to the disposal of PHI maintained on photocopier hard drives.[7]

In addition to the $1,215,780 payment, the settlement included a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all ePHI.[8] Leon Rodriguez, OCR Director, stated that the settlement "illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent."[9]

Because the Affinity copier snafu happened in 2010, Affinity's breach analysis required a determination as to whether there was a "significant risk of financial, reputational, or other harm to the individual" due to the unauthorized disclosure of the PHI stored on photocopier hard drives.[10] The standard was arguably more lenient than the new standard put in place under the HIPAA/HITECH Omnibus Final Rule. Nevertheless, the sheer size of the breach and the likelihood that at least some of the images retained on the copier hard drives would have contained highly sensitive health and financial data all but required Affinity to reach the conclusion it did—that a breach had occurred and that it was required to self-report the issue to the OCR.

The Omnibus Final Rule, which had a compliance date of September 23, 2013, presumes all unauthorized uses or disclosures of PHI constitute a "breach" unless the covered entity or business associate demonstrates through a risk assessment that there is a "low probability that the PHI has been compromised."[11] The Omnibus Final Rule identifies four "objective" factors covered entities and business associates must consider when performing the required risk assessment:

- What was the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification?
- Who was the unauthorized person who used the protected health information or to whom the disclosure was made?
- Was the protected health information actually acquired or viewed?
- To what extent was the risk to the protected health information mitigated?

While it remains to be seen how the OCR will apply the new breach standard going forward, the change to the underlying presumption and move towards more objective factors is consistent with the increased enforcement efforts being undertaken across the board by HHS. With less leeway for covered entities and business associates to determine that a breach did not occur, it is critical to ensure that ePHI is properly managed at all times. Encryption is all but required with respect to ePHI. The Affinity settlement should be seen as a message to covered entities and business associates to, in the words of Director Rodriguez, "undertake a careful risk analysis to understand the threats and

vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information."[12]

Jennifer Mitchell is a Partner in the Health Care Practice Group and leads the firm's HIPAA Privacy and Security practice and initiatives. In her HIPAA practice, she works with clients to minimize the risk of privacy and data security issues, assisting with all aspects of HIPAA privacy and security compliance, governance, audits/investigations, breach analyses, training, and strategic planning. Jen provides health care regulatory and compliance guidance to her clients in areas such as the federal and state anti-kickback laws, Stark law, PPACA (health reform), Sunshine Act, Medicare Secondary Payer laws, pharmaceutical marketing rules, ADA standards, and other laws and regulations impacting her health care clients. She also handles complex litigation in both state and federal courts and has an active investigations practice.

Stacey Borowicz is a Partner in the Health Care Practice Group. Stacey brings with her more than a decade of front line experience in the health care industry as she acquired a rare set of skills as a medical researcher/scientist prior to entering the practice of law. Her experience in the health care representation is diverse and includes Medicare/Medicaid audit and overpayment appeals, voluntary disclosures, and refunds. Stacey also brings a wealth of experience in regulatory compliance (HIPAA, Stark, anti-kickback, anti-markup rule), analyses, investigations, and mitigation. Outside of the health care arena, Stacey concentrates on franchise law and assists clients with franchise agreements as well as disclosure compliance.

Matthew Arend focuses his practice on all aspects of HIPAA privacy and security compliance, as well as breach analyses and governance. He also routinely advises clients on compliance with federal and state anti-kickback laws, Stark law, Sunshine Act, Medicare Secondary Payer laws, pharmaceutical marketing rules, and other regulatory matters. Additionally, his thorough knowledge of the health care arena enables him to counsel clients through audits and investigations, as well as providing training and strategic planning counseling. Matt also handles business and fiduciary litigation matters at the trial court and appellate levels.

Simi Botic's health law experience is diverse and includes practice formation and acquisition, contract review and preparation, scope of practice issues, regulatory compliance, Medicare/Medicaid appeals and reimbursement, employment-related transactions, certificates of need, health care fraud issues, as well as health law litigation.

In addition to her work in the health care industry, Simi's practice also includes litigation experience.

---

[1]United States Department of Health and Human Services, Office for Civil Rights and Affinity Health Plan, Inc. Resolution Agreement (Aug. 14, 2013), *available here*.

[2] 45 C.F.R. pt. 160 and 45 C.F.R. pt. 164, subpts. A and D.

[3]*HHS Settles with Health Plan in Photocopier Breach Case*, HHS Press Release (Aug. 14, 2013), *available here*.

[4] *Id*.

[5] *Id*.

[6] *Id*.

[7] *Id*.

[8] *See* Resolution Agreement, *available here*.

[9] *See* Press Release, *available here*.

[10] *See* 74 Fed. Reg. 42740 (Aug. 24, 2009).

[11] *See* 78 Fed. Reg. 5566 (Jan. 25, 2013).

[12] *See* Press Release, *available here*.

1620 Eye Street NW
Washington, DC 20006-4010
Phone: 202-833-1100 Fax: 202-833-1105